Jurnal Manajemen Informatika. Volume 9 Nomor 01 Tahun 2018, 18-25

UJI FITUR INTRUSION PREVENTION PADA FIREWALL UNTANGLE DENGAN PENGUJIAN DOS DAN SSH BRUTE FORCE

Mokhamad Aguk Nur Anggraini
D3 Manajemen Informatika, Fakultas Teknik, Universitas Negeri Surabaya
anggapim215@gmail.com

Abstrak

Keamanan data pada suatu infrastruktur jaringan merupakan suatu hal yang sangat sensitif dan rawan, seperti halnya yang pernah terjadi [1]. Salah satu alternatif untuk menanggulangi hal tersebut yaitu dengan menggunakan teknologi *IPS (Intrusion Prevention System)* dimana teknologi tersebut merupakan pengembangan dari *IDS (Intrusion Detection System)* yang menggunakan *Snort.* Banyak cara untuk menerapkan teknologi *IPS* salah satunya yang dilakukan pada [2]& [3]. Pada penelitian ini menerapkan teknologi *IPS* menggunakan *Firewall Untangle* dimana pada *platform* tersebut telah tersedia fitur *Intrusion Prevention* dengan maksud untuk menguji fitur tersebut pada *Firewall Untangle.* Pengujian dilakukan menggunakan serangan *DoS (Denial Of Service)* dan *SSH Brute Force* dimana didapatkan hasil bahwa fitur *Intrusion Prevention* pada *Firewall Untangle* dapat mengenali kedua serangan tersebut dan dapat melakukan *blocking* terhadap serangan tersebut dengan menggunakan *rule* yang ditambahkan secara manual.
Kata Kunci: Keamanan Data, *Intrusion Prevention System (IPS), Snort, Firewall Untangle, DoS Attack, SSH Brute Force*

Abstract

Data security in network infrastructure is a sensitive and confidential issue, as happened in [1]. One approach to cope unwanted incident is IPS technology implementation which was developed from Snort-based IDS, and have become common in field as reported in [2] & [3]. These studies made use of IPS provided by Untangle's Firewall and inspired this study to perform further observation. In this study, experiments have been done by creating several DoS, and SSH Brute Force attack. According to the results, Untangle is able to ackowledge and take required steps to handle the situation..
Keywords: Data Security, IPS, Snort, Untangle's Firewall, DoS, SSH Brute Force

PENDAHULUAN

Keamanan data pada suatu sistem jaringan merupakan suatu hal yang paling sensitif dan rawan, terutama bagi instansi-instansi besar yang membutuhkan keamanan data yang lebih aman. Contoh nyata serangan jaringan yang pernah terjadi yaitu diserangnya *Website* Telkomsel beberapa waktu lalu dengan cara *Web Defacing* atau dapat dikatan dibobolnya web lalu isi tampilan dari web tersebut diubah [1]. Selain itu, contoh kecil yang sering terjadi pada sistem jaringan yaitu usaha dari sekelompok orang untuk membobol suatu hak akses seperti *username* dan *password* dari suatu sistem jaringan, tentunya hal seperti itu sangat tidak diinginkan dan merugikan pemilik jaringan karena dapat mengganggu bahkan merusak kinerja dari jaringan itu sendiri.

Banyak alternatif cara untuk melakukan pencegahan terhadap serangan-serangan pada jaringan komputer salah satunya yaitu menerapkan teknologi *Intrusion Prevention System (IPS)*, dimana teknologi tersebut merupakan pengembangan dari *IDS (Intrusion Detection System)* yang menggunakan *Snort.* Teknologi ini memungkinkan untuk mengetahui adanya serangan dan melakukan pencegahan terhadap serangan tersebut dimana bekerja berdasarkan *rule* yang diterapkan. Tiap jenis serangan yang ingin dideteksi dan ditanggulangi diterapkan melalui *rule-rule* yang didefiniskan pada sistem *snort.*

Penerapan teknologi *IPS* juga mempunyai banyak cara seperti yang telah dilakukan pada studi [2] & [3], pada studi tersebut menerapkan tekonologi *IPS* dengan menginstall *snort* dan menerapkan *ip tables* pada *linux.* Namun belum banyak yang menerapkan teknologi *Intrusion Prevention System* menggunakan *Firewall Untangle.* Pada *Firewall Untangle* terdapat banyak fitur untuk membantu mengamankan sistem jaringan yang dibangun, salah satunya adalah fitur *Intrusion Prevention.* Eksistensi fitur ini menarik penulis untuk mengetahui bagaimana *Intrusion Prevention* bekerja pada *Firewall Untangle.* Dalam pengujian yang dilakukan, penulis memilih *DoS Attack* dan *SSH Bute Force,* pengujian tersebut dipilih karena kedua serangan tersebut merupakan serangan yang sangat umum dilkakukan dan cukup mudah untuk diterapkan, meskipun begitu dampak dari kedua serangan tersebut juga sangat buruk dimana *DoS Attack* dapat merusak sistem dengan cara membanjiri paket pada sistem dan *SSH Brute Force* merupakan serangan untuk

mengetahui hak akses dari sebuah sistem.

Tujuan dilakukannya uji fitur *Intrusion Prevention* pada *Firewall Untangle* ini yaitu untuk mengetahui bagaimana *Intrusion Prevention* pada *Firewall Untangle* bekerja, dan juga agar mengetahui hasil dari pengujian yang dilakukan. Lalu manfaat dilkaukannya uji fitur *Intrusion Prevention* pada *Firewall Untangle* ini yaitu agar sistem keamanan jaringan menjadi lebih baik dan mendapatkan gambaran dari performa *Firewall Untangle* pada fitur *Intrusion Prevention.*

KAJIAN PUSTAKA

Penelitian Terdahulu

Studi dalam bidang implementasi teknologi *Intrusion Prevention System* telah terdapat pada literatur terdahulu. Literatur-literatur tersebut melakukan sebuah implementasi teknologi *Intruion Prevention System* dimana pada umumnya melakukan uji coba menggunakan perangkat lunak *snort* yang dipasang pada sistem operasi *linux.* Penulis pada aritkel [2] menerapkan teknologi *Intrusion Prevention System* dengan cara melakukan pemasangan perangkat lunak *snort* pada sistem operasi *Linux* dimana *snort* berfungsi sebagai *Intrusion Detection System* lalu tindakan pencegahannya atau *Prevention* dilakukan dengan cara implementasi teknologi *IP Tables* pada *Linux* dimana juga terdapat teknologi *Fail2Ban* yang diimplementasikan.

Selain menggunakan perangkat lunak *snort* dalam penerapan *Intrusion Prevention System*, juga terdapat perangakat lunak lain yang difungsikan sebagai *Intrusion Detection System* yaitu *Suricata.* Pada artikel [3] menerapkan teknologi *Intrusion Prevention System* berbasis perangkat lunak *Suricata* dengan *IP Tables* pada *Linux*, yang dimana penerapannya dilengkapi dengan tampilan *Gudie User Interface* sebagai media monitoring apabila ada serangan yang terdeteksi. Dari kedua artikel [2]& [3] dalam menerapkan teknologi *Intrusion Prevention System* juga menggunakan suatu *Rule* yang ditambahkan untuk melakukan pencegahan terhadap suatu serangan.

Pada sisi pengujian serangan, artikel [2]& [3] menggunakan jenis serangan *DoS Attack*, dimana seperti pada artikel [4] membahas analisis sebuah serangan *DoS (Denial Of Service). DoS* sendiri merupakan aktifitas yang dapat menghambat kerja sebuah sistem komputer utamanya layanan (*service)*, sehingga pengguna yang berekepentingan dan berhak tidak dapat lagi menggunakan layanan tersebut [5]. Menurut artikel [4] ada banyak jenis serangan *DoS* yaitu *SYN Flooding, Pentium FOOF Bug, Ping Flooding, Apache Benchmark,* Menggantung *Socket, Input Flooding Attack, LAND Attack, Smurf Attack*, dan *Tear Drop.* Serangan yang sering menyerang layanan pada *server* yaitu *SYN Flooding* dimana serangan tersebut menyerang konek *TCP* yang terbentuk dengan membanjiri permintaan paket sehingga *server* tidak dapat membalas semua permintaan dan ahirnya *server down* dan layanan pun menjadi tidak dapat di akses.

Keamanan Jaringan

Keamanan Jaringan dapat diartikan sebagai keadaan aman pada suatu susunan yang menjalankan sistem komputer [6]. Keamanan jaringan juga dapat diartikan sebagai proses untuk mengidentifikasi dan mencegah adanya *user* yang tidak mempunayi izin (penyusup) dari sistem jaringan komputer. Tujuan dibangunnya suatu sistem keamanan jaringan adalah untuk menanggulangi dan mencegah ancaman dari jaringan luar yang dapat berupa ancaman logik atau fisik. Ancaman logik adalah sebauh ancaman yang berupa pengambilan data secara tidak saha atau pencurian data oleh penyusup dengan cara mencari celah yang terbuka pada sistem keamanan jaringan, sedangkan ancaman fisik yaitu sebuah ancaman yang berujuan untuk merusak sistem jaringan dari sisi *hardware* sebuah komputer.

Keamanan jaringan dalam aspek keamanan mempunyai 5 aspek yang dijelaskan sebagai berikut [7]:

1) *Confidentiality* yaitu mengharuskan suatu data hanya bisa diakses oleh pengguna yang sah atau memliki izin akses.
2) *Integrity* yaitu mengharuskan suatu data hanya bisa dirubah oleh pengguna yang sah atau memiliki izin wewenang.
3) *Availability* yaitu mengharuskan informasi hanya tersedia bagi pengguna yang sah atau memiliki izin akses untuk kebutuhan tersebut.
4) *Authentication* yaitu mengharusan penerima atau pengirim suatu data dapat dibuktikan dengan identitas yang asli dan tidak palsu yang dapat diidentifikasi.
5) *Nonrepudiation* yaitu mengharuskan penerima atau pengirim suatu data tidak dapat menolak adanya pengiriman dan penerimaan pesan.

Untangle

Untangle adalah suatu sistem operasi yang dirancang khusus untuk difungsikan sebagai *Firewall*, sehingga *Untangle* ini telah dilengkapi dengan aplikasi-aplikasi bawaan yang berufngsi sebagai *Firewall* yang sangat dibutuhkan untuk sistem jaringan [9]. *Untangle* juga bisa disebut *NG Firewall,* dimana *Untangle* ini berbasis sistem operasi *linux* tepatnya *linux debian* dengan dilengkapi aplikasi pendukung *java*. *Untangle* dapat dijadikan pilihan yang bijak baik bagi yang baru memulai maupun untuk keperluan profesional, karena *Untangle* menyediakan kofigurasi dengan melalui *web interface.* Pilihan paket yang disediakan *Untangle* yaitu *Free, Education, Lite dan Premium*. *Untangle* sendiri juga dapat difungsikan sebagai *Router* atau *Bridge* dimana apabila berfungsi sebagai *Router* maka *Untangle* dapat mengatur lalu lintas jaringan dibawahnya, namun apabila difungsikan sebagai *Bridge* maka *Untangle* hanya berfungsi untuk meneruskan jaringan dimana melalui penyaringan pada *Untangle* terlebih dahulu tidak mengatur jaringan dibawahnya.

Intrusion Prevention System

Intrusion Prevention System (IPS) adalah sebuah sistem *software* atau *hardware* yang dapat bekerja sebagai monitoring trafik jaringan, mendeteksi aktivitas yang tidak diinginkan dan melakukan pencegahan*(prevent)* dini terhadap pencurian atau kejadian yang bisa menyebabkan jaringan menjadi tidak seperti sebagaimana seharusnya. *IPS (Intrusion Prevention System)* mengkombinasikan teknik *Firewall* dengan metode *intrusion detection system (IDS)*. Teknologi *IPS* ini dapat digunakan sebgai piranti untuk mencegah aktifitas yang tidak diinginkan yang hendak masuk ke sistem jaringan yang dibangun dengan memeriksa, merekam dan mencatat semua paket data yang datang serta mengenali paket dengan adanya sensor notifikasi atau pemberitahuan saat adanya serangan yang teridentifikasi. Jadi *IPS (Intrusion Prevention System)* bertindak layaknya *Firewall* yang dapat mengizinkan atau mencegah paket data yang masuk [10].

Secara khusus, *IPS (Intrusion Prevention System)* mempunyai 4 aspek utama, yaitu:

1) *Normalisasi Traffic*: yaitu menginterpretasikan trafik lalu lintas jaringan dan melakukan analisis terhadap paket yang kemudian disusun kembali, seperti halnya untuk fungsi *block* sederhana.
2) *Detection Engine*: yaitu mendeteksi trafik jaringan dengan melakukan *pattern matching* terhadap tabel acuan dengan respon yang baik dan sesuai.
3) *Service Scanner*: yaitu membangun suatu tabel acuan guna mengelompokkan informasi yang diinginkan.
4) *Traffic Shaper*: yaitu membentuk dan mengatur trafik lalu lintas jaringan.

DoS Attack

DoS merupakan singkatan dari *Denial Of Service*, dan *DoS Attack* dapat diartikan menjadi serangan *Denial Of Service*. *DoS Attack* adalah sebuah jenis serangan pada sistem komputer atau umunya *server* didalam sistem jaringan dengan cara menghabiskan tersedianya sumber daya (*resource)* yang dimiliki oleh sistem komputer tersebut sehingga menyebabkan komputer tersebut tidak dapat lagi untuk menjalankan fungsinya dengan baik dan benar, sehingga secara tidak langsung berusaha untuk mencegah pengguna(*client)* untuk mendapatkan akses layanan dari *server* atau sistem komputer yang telah diserang tersebut [11].

Terdapat banyak aplikasi *instant* yang dapat melakukan serangan *DoS Attack* salah satunya yaitu aplikasi *Slowloris.* Aplikasi *Slowloris* merupakan aplikasi *instant* yang dapat melakukan serangan *DoS Attack* dengan jenis serangan *Syn Flooding* secara cepat dengan mengirimkan ribuan paket ke dalam sistem jaringan komputer target, dengan begitu *resource* target akan penuh dan akan mengalami *downtime (*tidak dapat diakses).

SSH Brute Force

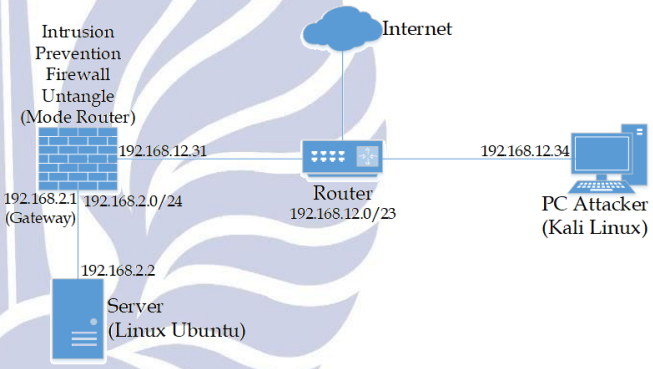
SSH Brute Force secara harfiah mempunyai arti serangan *SSH* secara paksa, dimana mempunyai arti sebuah aktifitas untuk terus menggali sebuah informasi secara terus menerus. Layanan *SSH* dapat memungkinkan pengguna jaringan untuk mengakses sebuah komputer dari jarak jauh dengan aman [12], dan tujuan *SSH Brute Force* yaitu untuk mengetahui hak akses berupa *username* dan *password* dari sebuah sistem yang ingin dibajak melalui protokol *SSH.*

Terdapat banyak aplikasi *exploit* salah satunya yaitu *Metasploit*, dengan aplikasi *Metasploit* maka *attacker* akan lebih mudah untuk mendapatkan hak akses dengan cara menyiapkan sebuha list data yang berisi *username* dan *password* yang didasarkan intensitas penggunaan secara umum dan juga tebakan-tebakan dari *attacker* itu sendiri.

METODE

Arsitektur Sistem

Pada tahapan ini, penulis akan menggambarkan dan menjelaskan mengenai *Firewall Untangle* dan topologi jaringan yang digunakan. Berikut adalah topologi jaringan yang digunakan:

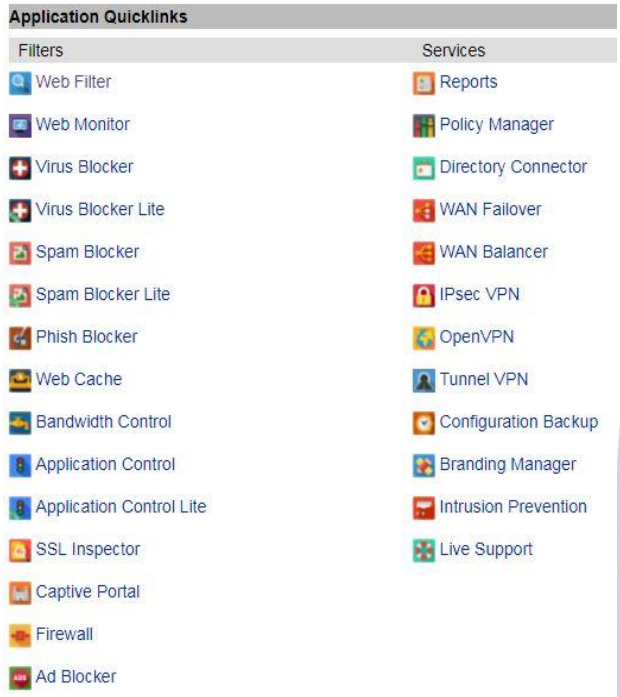


Gambar 1. Topologi Jaringan

Berikut penjelasan dari topologi jaringan diatas:

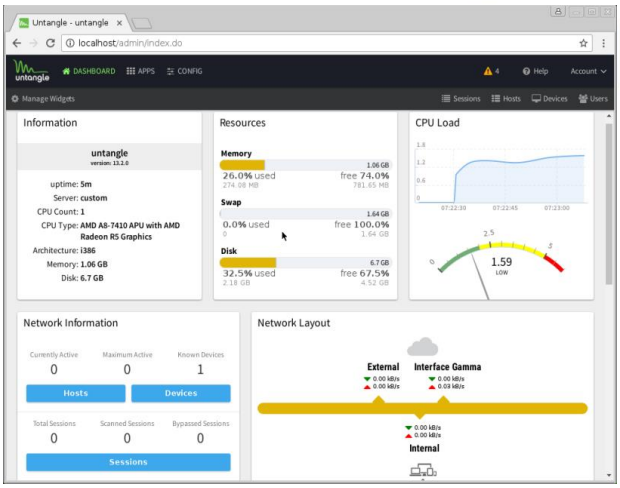
1) *Router* menerima jaringan Internet dari pusat yang telah dikelola dimana telah dikonfigurasi dengan memberikan *IP Address* 192.168.12.0/23 yang diberikan pada jaringan dibawahnya.
2) *Untangle Firewall* dengan fitur *Intrusion Prevention* di konfigurasi pada mode *Router* dimana terhubung pada *Router* dan mendapatkan *IP Address* 192.168.12.32 dan juga dikonfigurasi untuk memberikan *IP Address* pada jaringan dibawahnya dengan *IP Address* 192.168.2.0/24.
3) *Linux Ubuntu* sebagai *Server* terhubung pada *Untangle Firewall* dan perangkat jaringan dikonfigurasi dengan *IP Address* 192.168.2.2.
4) *PC Attacker* menggunakan sistem operasi *Kali Linux* terhubung pada *Router* dan diberikan *IP Address* 192.168.12.34 dimana yang telah terpasang aplikasi *Slowloris* untuk melakukan serangan *DoS* dan aplikasi *Metasploit* untuk melakukan *SSH Brute Force.*

Selanjutnya yaitu mengenai *Firewall Untangle* yang digunakan. *Firewall Untangle* yang digunakan pada penilitian ini yaitu *V.14.0 32bit* yang merupakan versi terbaru saat dilakukannya penelitian ini. Pada *Firewall Untangle* juga mempunyai banyak fitur yang dapat dimanfaatkan, berikut adalah fitur pada *Firewall Untangle*.



Gambar 2. Fitur *Firewall Untangle*

Dari sekian banyak fitur yang ada, yang akan diterapkan dan diujikan pada penelitian ini yaitu fitur *Intrusion Prevention*. Selain mempunyai banyak fitur, pada penerepan *Firewall Untangle* juga mempunyai 2 mode dalam penerapannya yaitu *Bridge* dan *Router* yang pada penelitian ini menggunakan mode *Router*. Dalam hal pelaporan sebuah *log* yang terjadi pada sistem, *Firewall Untangle* juga mempunyai tampilan *Dashboard* yang dapat dikonfigurasi untuk menampilkan *log* atau *accident* pada sistem. Berikut adalah tampilan *dashboard* dari *Firewall Untangle*.

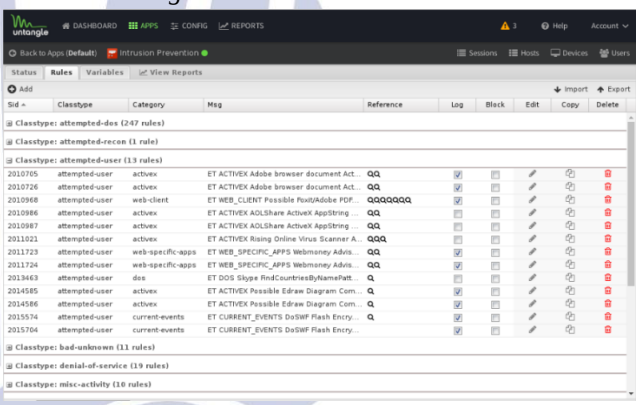


Gambar 3. *Dashboard Firewall Untangle*

Pada *Firewall Untangle* juga dapat melakukan *alert* atau pemberitahuan sebuah *log* melalui *email* dimana hal tersebut dapat memudahkan seorang adminsitrator dalam mengamati sistem yang ada. Dalam *dashboard* juga dapat ditampilkan *log* dari fitru yang aktif, dan berikut adalah contoh tampilan *log* saat *Intrusion Prevetion* megenali sebuah serangan yang juga ditampilkan di *dashboard*.

Gambar 4. *Log Intrusion Prevention*

Dalam fitur *Intrusion Prevention* yang ada pada *Firewall Untangle* terdapat banyak *rule* yang telah disediakan oleh *Firewall Untangle* dimana pengguna juga dapat menambahkan sebuah *rule* baru untuk diterapkan. Berikut tampilan sebagian katalog *rule* yang disediakan *Firewall Untangle*.

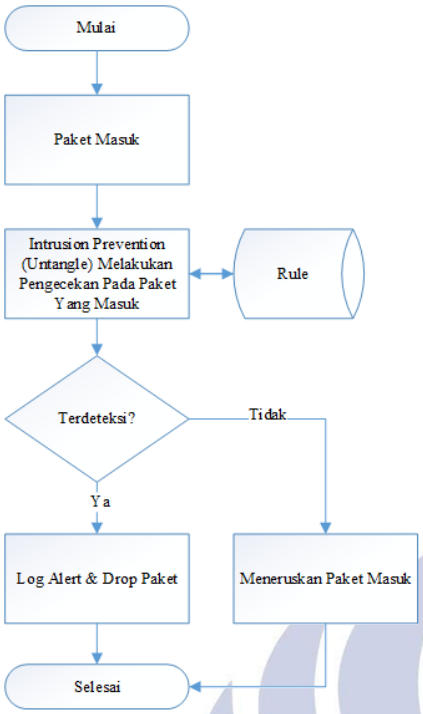


Gambar 5. *Rule Intrusion Prevention*

Katalog *rule* yang disediakan *Firewall Untangle* tersedia sangat banyak, dan juga dapat dilakukan penambahan *rule* yang dimana penulisan *rule* mengacu pada aturan dari *snort*. Aturan penulisan *rule* pada *Firewall Untangle* hanya terbatas dengan 2 *rule action* yaitu *alert* dan *drop* dimana sebenarnya pada aturan *snort* tidak hanya 2 *rule action* tersebut. Berikut form pengisian *rule* pada *Firewall Untangle:*

Gambar 6. Form Pengisian *Rule*

Sistem kerja dari *Intrusion Prevention* dapat digambarkan sebagai berikut.



Gambar 7. Sistem Kerja *Intrusion Prevention*

Pada gambar 7 menunjukkan sistem kerja *Intrusion Prevention* dimulai dengan datangnya paket masuk menuju *server* dari sistem jaringan yang dibangun, saat paket masuk kedalam jaringan selanjutnya *Firewall Untangle* tepatnya fitur *Intrusion Prevention* melakukan pengecekan paket tersebut berdasarkan *rule* yang telah diaktifkan, apabila paket yang masuk cocok dengan *rule* yang telah diaktifkan maka paket tersebut akan terdeteksi sebagai sebuah serangan dan akan ditampilkan sebuah *log alert* dimana juga dikirimkan lewat *email* dan paket akan di *drop/block*, apabila paket tidak terdeteksi dengan *rule* yang aktif maka paket akan diteruskan untuk masuk menuju *server*.

HASIL DAN PEMBAHASAN

Skenario Pengujian

Dalam uji coba yang dilakukan pada implementasi ini yaitu menggunakan *Firewall Untangle V.14.0 32bit* yang diimplementasikan dengan jaringan lokal pada Laboratorium Multimedia Kreatif Teknik Informatika Universitas Negeri Surabaya, dan menggunakan 2 PC dimana PC1 digunakan sebagai *Firewall Untangle* dan *Linux Ubuntu* sebagai *Server* yang dipasang secara *Virtual* dan PC2 digunakan sebagai PC *Attacker* yang menggunakan sistem operasi *Kali Linux* yang juga dipasang secara *Virtual*. Pada *Firewall Untangle* fitur yang diterapkan yaitu fitur *Report* dan *Intrusion Prevention*. Fitur *Report* merupakan fitur yang berfungsi untuk melaporkan semua *Report* yang ada pada *Firewall Untangle* termasuk laporan dari fitur-fitur yang terpasang. Fitur *Intrusion Prevention* nempunyai sistem kerja dimana bekerja berdasarkan *rule* yang diterapkan.

Skenario pengujian yang dilakukan yaitu mengacu pada topologi jaringan yang telah dibangun yaitu serangan *DoS Attack* dan *SSH Brute Force*. *DoS Attack* dilakukan pada *PC Attacker* dengan menggunakan aplikasi *Slowloris* yang merupakan serangan *DoS* berjenis *Syn Flooding*. Tahapan serangan yang dilakukan yaitu pada aplikasi dengan memasukkan *IP* dari *server* target dan selanjutnya *Slowloris* akan otomatis melancarkan serangan tersebut. Pada sisi *Untangle* diterapkan sebuah *rule* yang diisikan pada fitur *Intrusion Prevention*, *rule* yang diterapkan mengacu autran dari *Snort*. Untuk serangan *DoS* diterapkan *rule* sebagai berikut:

```
alert/drop tcp any any -> $HOME_NET $HTTP_PORTS ( msg: "TCP DOS"; flags: S; flow :stateless; threshold: type both, track by_src, count 70, seconds 10; sid: 1630; classtype: attempted-dos; )
```

Penjelasan dari *rule* diatas yaitu:

- *alert/drop* merupakan sebuah *action rule* dimana apabila yang diaktifkan *alert* maka aksi hanya melaporkan notifikasi dan apabila *drop* maka aksi yang dilakukan yaitu melakukan *block* pada paket yang masuk.
- *tcp* merupakan jenis protokol dari paket.
- *any any -> $Home_Net $HTTP_Ports* merupakan alur datangnya sumber paket menuju target, dimana pada *rule* ini sumber paket ditentukan dari mana saja dan taget menuju *Home_Net* tepatnya pada *HTTP_Ports*.
- *msg* merupakan pesan yang ditampilkan saat adanya notifikasi *log*.
- *flags* merupakan penentuan jenis paket dimana didefinisikan *S* yaitu paket *Syn*.
- *flow* merupakan aturan dari arus paket tertentu dimana didefinisikan *stateless* yaitu aturan untuk paket yang menyebabkan mesin mengalami *crash*.
- *threshold* merupakan merupakan batas dari *rule* yang digunakan dimana didefinisikan *type both* yaitu melihat kejadian pada satu interval, *track by_src* yaitu dilacak dari sumber alamat, *count* yaitu jumlah terjadinya *log* untuk paket yang ditentukan (70), dan *seconds* yaitu hitungan waktu dari jumlah paket yang ditentukan (10) pada *count*.
- *sid* merupakan *signature id* dari *rule* yang diterapkan.
- *classtype* merupakan pengelompokan tipe *rule* yang diterapkan.

Selanjutnya serangan *SSH Brute Force* juga dilakukan pada *PC Attacker* dengan menggunakan aplikasi *Metasploit* dimana aplikasi tersebut telah terpasang pada sistem operasi *Kali Linux*. Tahapan serangan yang dilakukan yaitu dengan menyiapkan *dictionary file* yang berisi perkiraan dari kombinasi *username* dan *password* dan aplikasi *Metasploit* menjalankan *dictionary file* tersebut untuk diujikan pada *server* target dengan memasukkan *IP* target. Pada sisi *Untangle* juga diterapkan sebuah *rule* yang diisikan pada fitur *Intrusion Prevention*, *rule* yang diterapkan mengacu

autran dari *Snort*. Untuk serangan *SSH Brute Force* diterapkan *rule* sebagai berikut:

```
alert/drop tcp any any -> $HOME_NET 22 ( msg: "Possible SSH Brute Forcing"; flags: S+; flow :stateless; threshold: type both, track by_src, count 3, seconds 10; sid: 1321; classtype: shellcode-detect; )
```

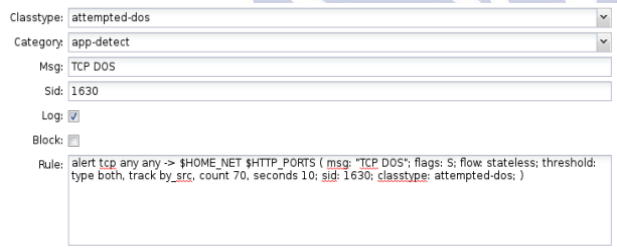
Penjelasan *rule* diatas hampir sama dengan *rule* pada *DoS Attack* hanya perbedaan pada target *port* yaitu menuju *port 22*, lalu *flags* menggunakan *S+* yang berarti *Syn* dengan bit yang ditentukan, dan *count* 3 dengan *seconds 10*.

Hasil Pengujian Dan Pembahasan

Berdasarkan rancangan skenario pengujian yang telah bitentukan, maka berikut pengujian yang telah dilakukan:

a) *DoS Attack* menggunakan aplikasi *Slowloris*

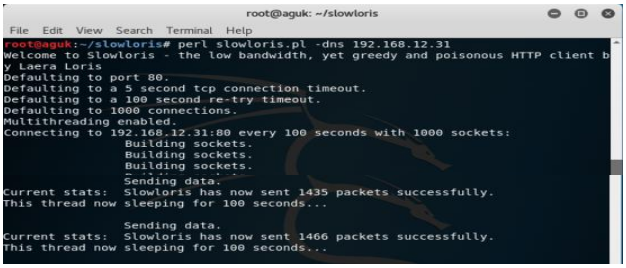
DoS Attack menggunakan *Slowloris* merupakan sebuah jenis serangan berjenis *Syn Flooding* yang mengarah pada *Server* yaitu *Port 80* dimana jenis serangan yang dilakukan yaitu mengirimkan ribuan paket secara langsung sehingga resource dari *Web Server* menjadi penuh dan mengakibatkan *Web Server* menjadi lambat bahkan tidak dapat diakses. *Rule* ditambahkan secara manual dan berikut *rule* yang diterapkan untuk *DoS Attack*:



Gambar 8. *Rule DoS Attack*

Pada gambar 8 merupakan *rule* yang diterapkan untuk *DoS Attack* dimana diisikan pada *field* yang telah disediakan pada *Firewall Untangle*, dan dapat dilihat bahwa aturan penulisan *rule* utamanya pada jenis *rule action* hanya terbatas *alert* dan *block* yang dimana sebenarnya dalam *snort* masih terdapat *rule action* lain yang dapat diterapkan sehingga penulisan *rule* pada *Firewall Untangle* menjadi terbatas.

Selanjutnya yaitu dilakukan penyerangan sebagai berikut:



Gambar 9. *DoS Attack* Dengan *Slowloris*

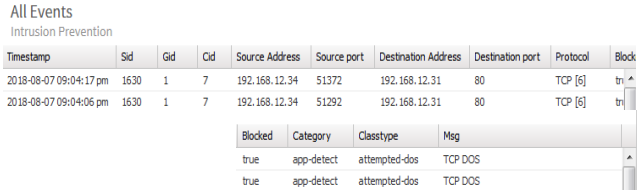
Pada gambar 9 dimasukkan perintah pada aplikasi *Slowloris* untuk melakukan serangan yaitu "`perl slowloris.pl -dns 192.168.12.31`" dimana perintah tersebut mengirim paket dengan *default* 1000 *connections* setiap 5 detik koneksi *tcp*. Dari penyerangan yang dilakukan, dapat dilihat bahwa *attacker* telah mengirimkan ribuan paket menuju *server* dan pada sisi *resource server* didapatkan hasil sebagai berikut:

Tabel 1. Hasil Resource Server

No.	Resource / Sumber Daya Server		Sebelum DoS	Saat DoS	Selisih
1.	CPU Core i7-7700 @3.8 GHz	Load Average Detik Terahir (%)	0,12	0,77	0,65
		Load Average 5 Detik Terahir (%)	0,09	0,23	0,14
		Load Average 15 Detik Terahir (%)	0,09	0,13	0,4
		Jumlah Tasks	184	324	140
2.	RAM	Total (KiB)	1015756		
		Free (KiB)	157084	86424	70660
		Used (KiB)	612152	692596	80444
		Buff (KiB)	246520	236736	9784
3.	SWAP	Total (KiB)	1046524		
		Free (KiB)	949120	922340	26780
		Used (KiB)	97404	124184	26780
		Available (KiB)	227308	127644	99664

Pada tabel 1 dapat dilihat bahwa aktifitas *CPU* pada *Server* saat dilakukan serangan *DoS* yaitu meningkat dari segi *Load Average* dan jumlah *Tasks* dimana jumlah *Tasks* meningkat hampir 2x lipat sebelum dilakukan *DoS*, begitu juga pada sisi *RAM* dimana terlihat perubahan yang cukup signifikan dari kondisi sebelum dilakukan *DoS* dan saat dilakukan *DoS* yang dimana sebelum *DoS* kondisi *RAM Free* masih 157084KiB dan *Used* sebesar 612152KiB dan saat dilakukan *DoS* kapasitas *Free* menjadi 86424KiB dan *Used* 692596KiB sehingga hal tersebut menjadikan *RAM* menjadi penuh dan menyebabkan *Resource* menjadi tidak dapat bekerja secara maksimal. Begitu juga dapat dilihat pada kondisi *SWAP* dimana tidak terjadi perubahan yang cukup signifkan karena *SWAP* hanya sebagai memori cadangan apabila *RAM* menjadi penuh.

Setelah *DoS* berhasil diterapkan, selanjutnya yaitu pada sisi *Firewall Untangle* didapatkan hasil sebagai berikut:



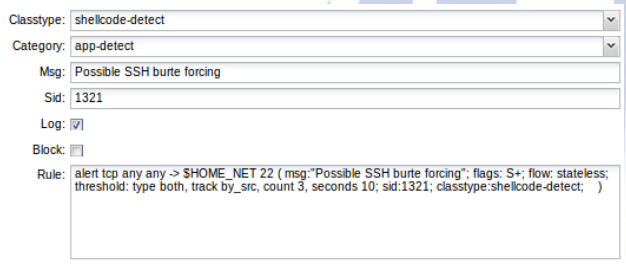
Gambar 10. *Events DoS Attack*

Pada gambar 10 merupakan *Events DoS Attack* yang berhasil dideteksi dimana hal tersebut juga berhasil dikirimkan dengan notifikasi melalui *email*. Hasil setelah *Block Rule* diaktifkan yaitu *IPS* berhasil melakuakn *Block* serangan namun menutup *port 80* secara keseluruhan sehingga hanya difungsikan sebagai *detection* saja.

b) *SSH Brute Force* menggunakan aplikasi *Metasploit*

SSH Brute Force merupakan sebuah usaha untuk menyerang sebuah *SSH Server* dengan tujuan untuk mendapatkan *username* dan *password* sehingga mempunyai akses untuk masuk pada *SSH Server* yang akan diserang. *SSH Brute Force* menyerang *SSH Server* dengan cara eksploitasi sebuah *username* dan *password* dengan cara menebak dengan *username* dan *password* yang telah disiapkan yaitu sebuah kumpulan *username* dan *password* yang sering digunakan secara umum seperti *root, admin, server* dll.

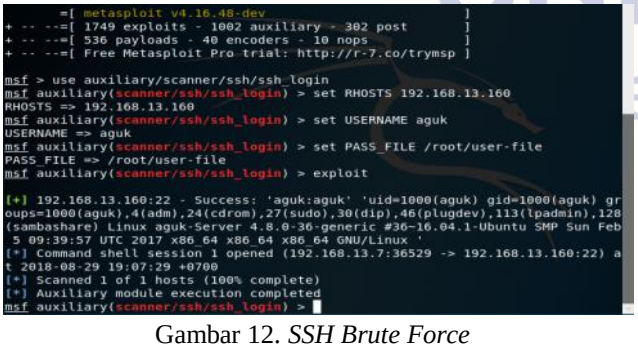
Pada pengujian ini, *rule default* dari *Firewall Untangle* tidak mengenali serangan ini sehingga ditambahkan *rule* baru sebagai berikut:



Gambar 11. *Rule SSH Brute Force*

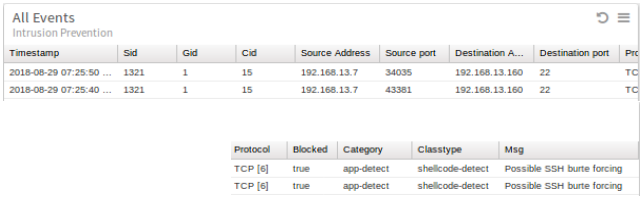
Pada gambar 11 merupakan *rule* yang diterapkan untuk *SSH Brute Force*, dan sepert yang dijelaskan sebelumnya yaitu aturan penulisan *rule* utamanya pada jenis *rule action* hanya terbatas *alert* dan *block* yang dimana sebenarnya dalam *snort* masih terdapat *rule action* lain yang dapat diterapkan sehingga penulisan *rule* pada *Firewall Untangle* menjadi terbatas.

Selanjutnya yaitu dilakukan penyerangan sebagai berikut:



Gambar 12. *SSH Brute Force*

Pada gambar 12 dilakukan penyerangan dengan memasukkkan perintah "`set PASS FILE /root/user-file`" dimana bertujuan untuk menjalankan *dictionary file* yang sudah disiapkan menuju *IP Server* target. Dari penyerangan yang dilakukan telah didapatkan hasil sebagai berikut:



Gambar 13. *Events SSH Brute Force*

Pada gambar 13 merupakan *Events SSH Brute Force* yang berhasil dideteksi dimana hal tersebut juga berhasil dikirimkan dengan notifikasi melalui *email*. Hasil setelah *Block Rule* diaktifkan yaitu *IPS* berhasil melakuakn *Block* serangan namun menutup *port 22* secara keseluruhan sehingga hanya difungsikan sebagai *detection* saja.

PENUTUP

Simpulan

Fitur *Intrusion Prevention* pada *Firewall Utangle* dapat dijadikan sebagai salah satu pilihan dalam menerapkan teknologi *Intrusion Prevention System* dimana penerapannya lebih mudah karena telah terintegrasi dengan *Firewall Untangle* tanpa harus melakukan pemasangan secara manual. Hasil-hasil eksperimen yang didapatkan setelah melakukan semua implementasi dan pengujian yaitu *Firewall Untangle* dapat mengenali serangan *DoS Attack* dan *SSH Brute Force* dan dapat melakukan *blocking* terhadap serangan tersebut, namun *action block* menutup *port* secara keseluruhan sehingga hanya difungsikan sebagai *detection*, hal tersebut juga karena terbatasnya aturan penulisan *rule* utamanya *rule action*. *Firewall Untangle* juga mengenali serangan dengan mengirimkan *Alert* atau notifikasi melalui *Email*.

Saran

Saran untuk pengembangan dan penelitian selanjutnya yaitu menerapkan *Intrusion Prevention* pada *Firewall Untangle* terbaru pada yang akan datang, karena sangat mungkin akan ada pembaruan pada fitur *Intrusion Prevention*. Lalu menerapkan metode serangan lain, pengiriman notifikasi penyerangan melalui aplikasi sosial media agar lebih efisien dan juga penggunaan komponen keamanan jaringan yang lain agar dapat secara maksimal untuk melakukan pencegahan terhadap suatu serangan.

UCAPAN TERIMA KASIH

Ucapan terima kasih kepada **Bapak Ibnu Febry Kurniawan, S.Kom., M.Sc.** selaku Pembimbing untuk penelitian dan pengerjaan artikel ini.

DAFTAR PUSTAKA

[1] F. K. Bohang, “Situs Telkomsel Diretas, Berisi Keluhan Internet Mahal,” 2017. [Online]. Available: https://tekno.kompas.com/read/2017/04/28/08042477/situs.telkomsel.diretas.berisi.keluhan.internet.mahal. [Accessed 15 Maret 2018].

[2] Y. W. Pradipta, "Iplementasi Intrusion Prevention System (IPS) Menggunakan SNORT Dan IP Tables Berbasis Linux," *Jural Manajemen Informatika*, vol. VII, no. 1, pp. 21-28, 2017.

[3] D. Kuswanto, "Unjuk Kerja Intrusion Prevention Sistem (Ips) Berbasis Suricata Pada Jaringan Lokal Area Network Laboratorium Tia+ Teknik Informatika, Universitas Trunojoyo," *Jurnal Ilmiah NERO*, vol. I, no. 2, pp. 73-81, 2014.

[4] J. J. Siregar, "Analisis Exploitasi Keamanan Web Denial Of Service Attack," *Comtech*, vol. IV, no. 2, pp. 1199-1205, 2013.

[5] M. L. Herlambang, Buku Putih Cracker: Kupas Tuntas DOS Attack + Cara Penanggulangannya, Yogyakarta: Andi Publisher, 2010.

[6] N. Abdiansyah, “Definisi Keamanan Jaringan Komputer,” 2013. [Online]. Available: https://nugi.biz/2013/05/05/definisi-keamanan-jaringan-komputer.xhtml. [Accessed 16 Maret 2018].

[7] F. Seventeen, “Aspek Yang Meliputi Sistem Keamanan Jaringan Komputer,” 2016. [Online]. Available: https://www.galitekno.com/2016/10/aspek-yang-meliputi-sistem-keamanan.html. [Accessed 15 Maret 2018].

[8] R. Towidjojo, Mikrotik Kungfu, Ke-1 ed., Jakarta: Jasakom, 2016.

[9] N. Abdiansyah, “Untangle Platform Management Part 1 : Introduction,” 2013. [Online]. Available: https://nugi.biz/2013/05/19/untangle-platform-management-part-1-introduction.xhtml. [Accessed 15 Maret 2018].

[10] R. Alder, "Snort 2.1 Intrusion Detection, Second," Rockland, MA 02370, 2004.

[11] Anas, "Pengertian DDoS Attack, DoS Attack dan Cara Kerjanya," 2018. [Online]. Available: teknologiraf.com/pengertian-ddos-attack/. [Accessed 5 September 2018].

[12] Admin, "Pengertian dan Mnafaat SSH Bagi Developer," 2016. [Online]. Available: hhttps://idcloudhost.com/pengeritan-dan-manfaat-ssh-bagi-developer/. [Accessed 5 September 2018].